



Rat der
Europäischen Union

Brüssel, den 18. Oktober 2023
(OR. en)

14394/23

COSI 181
CRIMORG 139
ENFOPOL 433
CT 156
COTER 186
AVIATION 194
JAI 1334

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	18. Oktober 2023
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2023) 659 final
Betr.:	MITTEILUNG DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT über die Abwehr potenzieller Bedrohungen, die von Drohnen ausgehen

Die Delegationen erhalten in der Anlage das Dokument COM(2023) 659 final.

Anl.: COM(2023) 659 final



EUROPÄISCHE
KOMMISSION

Brüssel, den 18.10.2023

COM(2023) 659 final

**MITTEILUNG DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE
PARLAMENT**

über die Abwehr potenzieller Bedrohungen, die von Drohnen ausgehen

I. EINFÜHRUNG

In dieser Mitteilung wird die EU-Politik zur Abwehr potenzieller Bedrohungen durch nicht kooperative unbemannte Luftfahrzeugsysteme (unmanned aircraft systems – UAS), gemeinhin als „Drohnen“ bezeichnet, dargelegt. Sie ist Teil eines umfassenderen Pakets zur Drohnenabwehr, das auch zwei Handbücher mit praktischen Anleitungen zu den wichtigsten technischen Aspekten dieser Politik umfasst. Dieses Paket wurde in der Mitteilung der Kommission „*Eine Drohnenstrategie 2.0 für ein intelligentes, nachhaltiges Ökosystem für unbemannte Luftfahrzeuge in Europa*“¹ als eine Leitinitiative angekündigt. Mit dieser Mitteilung wird den folgenden Erfordernissen Rechnung getragen: i) Schaffung eines umfassenden und harmonisierten politischen Rahmens, ii) Aufbau eines gemeinsamen Verständnisses der anwendbaren Verfahren, um den sich ständig wandelnden Bedrohungen zu begegnen, die von Drohnen ausgehen können, iii) Berücksichtigung der raschen technologischen Entwicklung.

A. Ergänzung des EU-Rahmens zu Drohnen

Die rechtmäßige Verwendung von Drohnen ist ein zentraler Aspekt bei der Umsetzung des grünen und des digitalen Wandels, wie in der „Drohnenstrategie 2.0“ der EU festgelegt. Drohnen sind insbesondere in den Bereichen Verkehr, Verteidigung, Handel und Dienstleistungen von Bedeutung. Die Zahl der in der EU eingesetzten Drohnen dürfte in den kommenden Jahren erheblich zunehmen, und in Bezug auf Geschwindigkeit, Wendigkeit, maximale Reichweite, Nutzlastkapazität, Präzision der Sensoren und Einsatz künstlicher Intelligenz sind erhebliche Verbesserungen zu erwarten. Diese Entwicklungen werden sich in einem breiteren Spektrum legitimer und rechtmäßiger Verwendungen von Drohnen niederschlagen. Damit dieses Potenzial ausgeschöpft werden kann, muss jedoch der potenziellen Bedrohung begegnet werden, die von nicht kooperativen Drohnen ausgehen kann. Die Definition einer nicht kooperativen Drohne richtet sich nach der Art der Nichtkooperation, die unter anderem kriminell, illegal (vorsätzlicher Regelverstoß) oder amateurhaft (aus Unwissenheit oder Leichtsinnigkeit) sein kann.

Die vorliegende Mitteilung befasst sich mit den Bedrohungen durch Drohnen, die für zivile Zwecke bestimmt sind, und soll dazu beitragen, von diesen Drohnen ausgehende Bedrohungen in einem zivilen Umfeld zu bekämpfen. Auch wenn der Schwerpunkt dieser Mitteilung nicht auf für Verteidigungszwecke konzipierten Drohnen liegt, so gibt es doch etliche Berührungspunkte mit dem Verteidigungsbereich. Dazu zählen die mögliche Verwendung kleinerer für Verteidigungszwecke konzipierter Drohnen durch Kriminelle oder Terroristen sowie die Synergien zwischen Drohnenabwehrtechnologien. Für Verteidigungszwecke konzipierte Drohnen könnten denselben Luftraum beanspruchen wie zivile Drohnen, und in diesen Fällen müssen sie von den zuständigen Behörden für die Lageerfassung identifizierbar sein.

In dieser Mitteilung geht es speziell um die *Abwehr* potenzieller Bedrohungen, die von Drohnen ausgehen. Dementsprechend soll darin nicht die weiter gefasste Dimension der Rolle von Drohnen im Bereich der inneren Sicherheit behandelt werden, d. h. deren Einsatz zu Zwecken der Strafverfolgung, der öffentlichen Sicherheit und der Gefahrenabwehr.

Für die Abwehr von Bedrohungen, die von nicht kooperativen Drohnen ausgehen, sind in erster Linie die Behörden der Mitgliedstaaten zuständig. Die Mitgliedstaaten profitieren jedoch auch von Maßnahmen auf EU-Ebene, die eine engere Zusammenarbeit und Koordinierung bei den verschiedenen hierzu

¹ Eine Drohnenstrategie 2.0 für ein intelligentes, nachhaltiges Ökosystem für unbemannte Luftfahrzeuge in Europa, COM(2022) 652 final vom 29. November 2022.

eingesetzten Mitteln und Instrumenten ermöglichen. Mit dieser Mitteilung werden daher verschiedene Maßnahmen im Zusammenhang mit dem Aufbau von Gemeinschaften und dem Informationsaustausch unterstützt. Außerdem werden die Mitgliedstaaten mit darin vorgesehenen Leitlinien, Schulungen, Finanzierungen und operativen Verfahren unterstützt.

Potenziell gefährliche Vorfälle mit Drohnen haben sowohl innerhalb der EU als auch außerhalb ihrer Grenzen zugenommen. Es ist daher von entscheidender Bedeutung, die Einführung physischer oder digitaler Lösungen zur Drohnenabwehr durch Strafverfolgungsbehörden und andere öffentliche Stellen in der EU sowie durch Betreiber kritischer Infrastrukturen zu erleichtern. Die Ausarbeitung einer EU-Politik zur Drohnenabwehr wird dazu beitragen, die Verfahren zur Prüfung der Effizienz verfügbarer neuer Lösungen zu verbessern und die gezielte Nutzung von Forschung und Innovation in diesem Bereich zu fördern. Mit der Entwicklung dieser Politik zur Drohnenabwehr trägt die Kommission zur Stärkung eines EU-Marktes für Drohnenabwehlösungen bei. Dies wird den Weg für eine größere strategische Autonomie und technologische Souveränität der EU – auch in Bereichen der kritischen Technologien – ebnen. Damit werden die europäischen Kapazitäten zur Entwicklung von Spitzenlösungen in den Bereichen Verteidigung, Luft- und Raumfahrt sowie zivile Sicherheit gefördert, und die Abhängigkeit von außereuropäischen Anbietern wird verringert. Als Grundlage dienen dabei die Ergebnisse der Bewertung der Abhängigkeiten im Bereich der kritischen Technologien², und es werden weitere Daten und Analysen bereitgestellt. Ferner wird damit i) das Verständnis der Kommission für den Einsatz kritischer Technologien und die Abhängigkeit von außereuropäischen Anbietern geschärft und ii) ein genauer Überblick über den Grad der Abhängigkeit gegeben.

Darüber hinaus ist es im Hinblick auf die Abwehr von Bedrohungen, die von nicht kooperativen Drohnen ausgehen, aus behördlicher Sicht auch wichtig i) über klare und harmonisierte Rahmen und Verfahren zu verfügen, ii) den zuständigen öffentlichen und privaten Akteuren die klare Befugnis zum Eingreifen gegen nicht kooperative Drohnen zu erteilen und iii) die Zusammenarbeit zwischen Interessenträgern zu erleichtern, die dies nicht immer gewohnt sind (Strafverfolgung, Zivilluftfahrtbehörden, Betreiber, Hersteller, Mobilfunknetzbetreiber). In dieser Mitteilung werden Maßnahmen vorgeschlagen, um i) zu einem allgemeinen Konsens über die Verfahren zu gelangen, die beim Umgang mit von Drohnen ausgehenden Bedrohungen zur Anwendung kommen sollen, und ii) zu ermitteln, inwieweit es einer Harmonisierung der Regulierungsmaßnahmen bedarf.

B. Bekämpfung einer aktuellen – und sich rasch wandelnden – Bedrohung

Sowohl in der EU-Strategie für eine Sicherheitsunion³ als auch in der Agenda für Terrorismusbekämpfung⁴ wird betont, dass die Bedrohung durch nicht kooperative Drohnen in Europa ein ernstes Problem darstellt.

Die rasch fortschreitenden Fähigkeiten von Drohnen stellen ein wachsendes Sicherheitsrisiko dar. In den letzten Jahren wurden Pläne aufgedeckt, Drohnen für Terroranschläge zu testen und einzusetzen.⁵ Es

² Eine 2022 durchgeführte kommissionsinterne eingehende Bewertung zu autonomen Systemen.

³ EU-Strategie für eine Sicherheitsunion, COM(2020) 605 final vom 24. Juli 2020.

⁴ Eine EU-Agenda für Terrorismusbekämpfung: antizipieren, verhindern, schützen, reagieren, COM(2020) 795 final vom 9. Dezember 2020.

⁵ Beispiele hierfür sind: i) der Plan eines überzeugten Dschihadisten, der im Oktober 2022 von einem spanischen Gericht verurteilt wurde, weil er einen Anschlag auf ein Stadion während eines wichtigen Fußballspiels mit einer mit Sprengstoff bestückten Drohne geplant hatte, und ii) ein belgischer Staatsangehöriger, der für einen versuchten Bombenanschlag mit Drohnen auf ein Gefängnis verurteilt wurde.

wurden auch verdächtige Drohnen in der Nähe von kritischen Infrastrukturen wie Energieanlagen, Flughäfen und Häfen gesichtet, was auf eine mögliche missbräuchliche Verwendung von Drohnen zur feindlichen Informationsbeschaffung hinweist. Drohnen werden von Kriminellen für den grenzüberschreitenden Schmuggel oder zur Erleichterung anderer illegaler Aktivitäten, einschließlich des Drogenhandels, eingesetzt. Außerdem können Drohnen Cyberrisiken bergen, wenn sie beispielsweise zur digitalen Aufklärung eingesetzt werden. Die von Drohnen ausgehenden Bedrohungen sind nicht bloß ein technisches Problem. Heute können die meisten für zivile Zwecke konzipierten Drohnen zwar entdeckt und identifiziert werden, es ist aber immer noch sehr schwierig, sie zu übernehmen oder zu neutralisieren (d. h., die Kontrolle über sie zu übernehmen, sie sicher zu landen oder sie abzuschießen), was oft auf das Fehlen einer entsprechenden rechtlichen Befugnis zurückzuführen ist. Dies gilt insbesondere für private Betreiber kritischer Infrastrukturen. Die Abwehr der von Drohnen ausgehenden Bedrohungen sollte daher bei künftigen Risikobewertungen im Rahmen der Richtlinie über die Resilienz kritischer Einrichtungen⁶ berücksichtigt werden.

Das Bedrohungsbild wird in Anbetracht von Vorfällen in Ländern nahe der EU und in anderen Teilen der Welt noch deutlicher. Drohnen haben sich als kostengünstige und wirkungsvolle Plattform mit doppeltem Verwendungszweck erwiesen, die im Krieg Russlands gegen die Ukraine Innovationen im Verteidigungsbereich vorangetrieben hat. Der Einsatz von für zivile Zwecke konzipierten Drohnen für zerstörerische Angriffe auch in anderen bewaffneten Konflikten (wie in Jemen oder Syrien) ist ein Phänomen, das sich wahrscheinlich auf die innere Sicherheit der EU auswirkt. Der modus operandi terroristischer Gruppen und die geschicktere Verwendung handelsüblicher Drohnen könnten unsere Grenzen erreichen und eine Bedrohung darstellen. Gleiches gilt für den Einsatz von Drohnen für gezielte Mordversuche.⁷

Lösungen zur Drohnenabwehr sind jedoch nicht nur gegen gezielte böswillige Nutzung erforderlich. Sie sind auch zur Verhinderung von Vorfällen notwendig, die durch Fahrlässigkeit oder Leichtfertigkeit verursacht werden. Die meisten Drohnenutzer in der EU (insbesondere lizenzierte professionelle Fernpiloten oder organisierte Freizeitpiloten) halten sich an die bestehenden Regeln, Vorschriften und technischen Beschränkungen. Unwissende, unachtsame und kriminelle Drohnenutzer sind jedoch für die zahlreichen gefährlichen Vorfälle mit Drohnen in der EU verantwortlich. Öffentliche Großveranstaltungen sind besonders anfällig für solche Störfälle, ebenso wie einige kritische Sektoren wie der Luftverkehr. Darüber hinaus kann der unrechtmäßige Einsatz von Drohnen auch die persönliche Sicherheit und das Recht auf Schutz der Privatsphäre von Einzelpersonen beeinträchtigen, insbesondere wenn Drohnen in Wohngebieten betrieben werden.

C. Schritthalten mit technologischen Entwicklungen

Der Schutz unserer Gesellschaften vor böswilligen und nicht kooperativen Drohnen erfordert den Zugang zu erschwinglichen und zuverlässigen Abwehrmaßnahmen, die flexible Lösungen ermöglichen. Die Lösungen betreffen in der Regel die drei Bereiche Erkennung, Verfolgung und Identifizierung, während die Behörden auch an zwei weiteren Aspekten interessiert sind: Neutralisierung und Forensik.

Im Bereich der Verteidigung wie auch der zivilen Sicherheit werden bereits innovative Lösungen zur Drohnenabwehr entwickelt und getestet. Ihr Markteintritt und ihre Übernahme durch die Endnutzer

⁶ Richtlinie (EU) 2022/2557 vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen (ABl. L 333 von 2022, S. 164).

⁷ Beispiele hierfür sind der gescheiterte Versuch, den venezolanischen Präsidenten zu ermorden, und der Einsatz von Drohnen durch mexikanische Drogenkartelle gegen Vertreter anderer krimineller Vereinigungen.

können durch einen übergreifenden EU-Rahmen zur Drohnenabwehr, wie er in dieser Mitteilung propagiert wird, erleichtert werden. Ein standardisierter Einheitsansatz für die Umsetzung von Drohnenabwehrmaßnahmen ist jedoch aufgrund der großen Vielfalt möglicher Einsatzszenarien und -umgebungen nicht möglich.

Die Maßnahmen zur Drohnenabwehr müssen daher an die unterschiedlichen Bedürfnisse und die verschiedenen Betriebsumgebungen angepasst werden. Aus Sicht der für die innere Sicherheit zuständigen Behörden kann in bestimmten Situationen die vollständige physische Zerstörung einer Drohne die bevorzugte und einzige Option sein, etwa um einen drohenden Angriff auf Menschen oder Infrastruktur zu verhindern. In anderen Fällen, z. B. bei krimineller Nutzung oder feindlicher Informationsbeschaffung, besteht ein großes Interesse daran, die Kontrolle über die Drohne zu erlangen, um sie möglichst unversehrt zu landen und so eine bestmögliche forensische Untersuchung zu ermöglichen. In diesem Zusammenhang bedarf es auch anspruchsvoller Cyber-Lösungen, mit denen das Betriebssystem einer Drohne unter Kontrolle gebracht werden kann.

Einer der technologischen Trends, der beobachtet und aktiv genutzt werden sollte, ist die Entwicklung von Sensoren für die genauere Erkennung von Drohnen. Die bestehenden Sensorfunktionen können weiterentwickelt werden, um eine Drohne nicht nur zu erkennen, sondern auch um die von ihr ausgehende Bedrohung durch die Analyse von Flugmustern, die Erkennung von Nutzlast und Ausrüstung zu bewerten. Sensoren und Erkennungssysteme müssen in der Lage sein, sich an die wechselnden Formen und Fähigkeiten von Drohnen anzupassen (Geschwindigkeit, Wendigkeit, Fähigkeit, Täuschkörper einzusetzen, usw.). Die Fähigkeit von Behörden und privaten Betreibern kritischer Infrastrukturen, Daten von diesen Sensoren zu analysieren, wird zunehmend an Bedeutung gewinnen. Auch künstliche Intelligenz wird eine Rolle spielen, z. B. durch die automatische Generierung von Warnungen, die Risikokalkulation, die Vorhersage von Flugrouten oder Landeplätzen. Neue Trends auf den Drohnenmärkten müssen daher kontinuierlich beobachtet und in Lösungen zur Drohnenabwehr einbezogen werden. Die Behörden in der EU sollten anhand der Beobachtung dieser technologischen Entwicklungen Prioritäten für Investitionen festlegen und die Entwicklungen unterstützen können, die am besten geeignet sind, die von den Strafverfolgungsbehörden der Mitgliedstaaten und privaten Betreibern geäußerten operativen Bedürfnisse zu erfüllen.

Was die Übernahme und Neutralisierung betrifft, so sind weitere Tests von Technologien erforderlich, die für verschiedene Umgebungen und Szenarien geeignet sind. Im Verteidigungsbereich wurden Lösungen gefunden, um eine Drohne in der Luft zu zerstören oder im Ganzen einzufangen, sodass weniger Trümmerteile entstehen, die zu Personen- oder Sachschäden führen könnten. Dazu zählen gerichtete Energie in Form von Hochleistungslasern sowie der Einsatz von Hochfrequenzsystemen, Systemen zum Abfangen mit Netzen und digitalen Tools, um die Kontrolle über nicht kooperative Drohnen zu erlangen.

Für die Strafverfolgung und die Ermittlungen wäre es besonders hilfreich, eine Drohnengefahr durch die Übernahme des Steuerungssystems zu neutralisieren und die Drohne sicher zu landen, um den Behörden und Ermittlern bestmöglichen Zugang zu potenziellen physischen und digitalen Beweismitteln zu ermöglichen. Daher sollte für den Bereich der inneren Sicherheit eine breite Palette verschiedener Lösungen für unterschiedliche Zwecke zur Verfügung stehen und validiert werden. Dementsprechend muss ein echtes Markt- und Innovationsumfeld für Lösungen zur Drohnenabwehr gefördert werden, die den Anforderungen des Bereichs der zivilen Sicherheit gerecht werden. Andernfalls ist es unwahrscheinlich, dass die Entwicklung von Lösungen zur Drohnenabwehr mit der wachsenden Zahl und den zunehmenden Fähigkeiten der Drohnen selbst Schritt halten wird. Außerdem ist es von entscheidender Bedeutung, diesen Markt zu strukturieren und zu segmentieren, um den betroffenen Behörden zu helfen, die für ihre Bedürfnisse am besten geeigneten Lösungen zu finden.

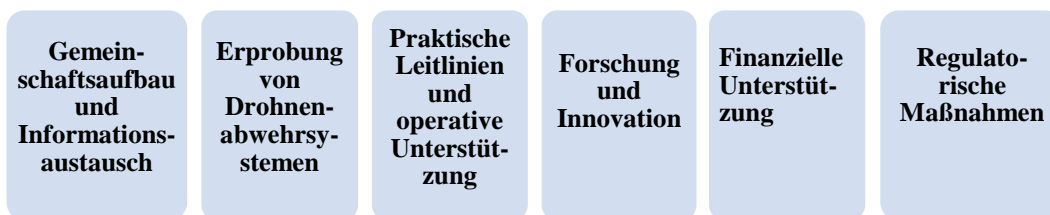
Darüber hinaus ist es wichtig, die von Kriminellen genutzten sogenannten Counter-Counter-Drone-Systeme (Anti-Drohnenabwehrsysteme) zu überwachen. Anti-Drohnenabwehrsysteme sind Vorrichtungen, die von der Drohne mitgeführt oder vom Boden aus eingesetzt werden und bestimmte Drohnenabwehrmaßnahmen unterlaufen sollen.

Schließlich werden viele Drohnenabwehrsysteme auch zu Verteidigungszwecken entwickelt. Auch wenn sie sich in ihren Anforderungen unterscheiden, weisen sie häufig gemeinsame Merkmale und Technologien mit Systemen für zivile Zwecke auf, weshalb eine enge Zusammenarbeit mit dem Verteidigungsbereich erforderlich ist.

Diese technologische Landschaft, die sich ständig weiterentwickelt, erfordert auch einen kohärenten und ständig aktualisierten Rechtsrahmen für den Einsatz von Drohnenabwehrsystemen.

II. GESTALTUNG EINER EU-POLITIK ZUR DROHNENABWEHR

Die Kommission beschäftigt sich seit 2016, als der erste EU-Workshop zur Drohnenabwehr stattfand, gemeinsam mit den Mitgliedstaaten und anderen Interessenträgern mit der potenziellen Bedrohung, die von Drohnen ausgeht. Seitdem wurde eine breite Palette von Initiativen ins Leben gerufen, um den Gemeinschaftsaufbau, den Informationsaustausch, die Entwicklung bewährter Verfahren und die gezielte Finanzierung von Projekten zu erleichtern. Die Kommission wird infolge der Gespräche mit den Sachverständigen der Mitgliedstaaten diese laufenden Initiativen weiter unterstützen und gleichzeitig neue Arbeitsbereiche weiterentwickeln und integrieren, um eine umfassende EU-Politik zur Drohnenabwehr zu entwickeln. Diese Arbeit umfasst die folgenden sechs Haupttätigkeiten:



A. Gemeinschaftsaufbau und Informationsaustausch

Ein breites Spektrum von Netzen und Akteuren arbeitet derzeit auf EU-Ebene an Lösungen zur Drohnenabwehr. Ihre künftigen Tätigkeiten müssen daher in politischer, technischer und operativer Hinsicht optimiert und gelenkt werden, um: i) funktionierende Gemeinschaften von Interessenträgern aufzubauen, ii) einen wirksamen Austausch von Informationen und bewährten Verfahren zu gewährleisten und iii) Doppelarbeit zu vermeiden.

Die Kommission wird bestehende Initiativen auf technischer Ebene unterstützen und gleichzeitig eine **Expertengruppe der Kommission zur Drohnenabwehr** einrichten, die auf politischer Ebene beratend tätig werden soll. Diese Expertengruppe kann strategischen Input für verschiedene politische Maßnahmen auf EU-Ebene mit Relevanz für die Drohnenabwehr liefern, z. B. in den Bereichen innere Sicherheit, Grenzschutz oder Resilienz kritischer Infrastrukturen. Dazu wird sie mit anderen Expertengruppen und gegebenenfalls mit den einschlägigen Arbeitsgruppen des Rates zusammenarbeiten.

Es finden regelmäßig Workshops und Expertensitzungen zu Drohnenabwehrlösungen und -strategien statt. Daran nehmen politische Entscheidungsträger, technische Experten und Forscher von Kommission, Mitgliedstaaten, anderen EU-Institutionen, EU-Agenturen, EU-finanzierten Projekten, internationalen Organisationen und Partnerländern teil. Mit diesen Aktivitäten wurde eine kontinuierliche Einbindung aller Interessenträger erreicht, was ihre operative und praktische Zusammenarbeit erheblich erleichtert hat. Dazu hat die Kommission das **Counter-UAS Information Hub**⁸ (Informationsportal zur Drohnenabwehr) eingerichtet, das derzeit über 300 Mitglieder zählt. Diese Online-Plattform, auf der verschiedene Informationsquellen wie die Ergebnisse einschlägiger EU-finanzierter Projekte, Präsentationen, Berichte und ein halbjährlicher Newsletter zu finden sind, wird regelmäßig aktualisiert.

Die Gemeinschaftsbildung und der Informationsaustausch, insbesondere im Hinblick auf die operativen Erfordernisse der Strafverfolgungsbehörden, finden zu einem großen Teil auch im Rahmen der von der EU finanzierten **Europäischen Strafverfolgungsnetze** statt. Alle folgenden Netzwerke haben beispielsweise eigene Maßnahmen zur Abwehr der von Drohnen ausgehenden Bedrohungen eingeleitet: das Europäische Netz technischer Dienste für die Strafverfolgung (ENLETS), das EU-Netz für Polizei- und Grenzschutzeinheiten auf Flughäfen (AIRPOL), das EU-Netz der Spezialeinheiten (ATLAS), das EU-Sicherheitsnetz für Hochrisikofälle. Die neu eingerichtete Arbeitsgruppe des Strafverfolgungsnetzes, eine von der Kommission⁹ finanzierte Initiative der GD HOME zur Förderung der Zusammenarbeit zwischen polizeilichen Netzen, wird die laufenden Arbeiten im Bereich der Drohnenabwehr in einer speziellen Unterarbeitsgruppe bündeln.

Die **Europäische Agentur für Flugsicherheit (EASA)** hat unverbindliche Leitlinien ausgearbeitet, die Behörden und Flughäfen dabei helfen, sich auf Drohnenfälle vorzubereiten, darauf zu reagieren und sich davon zu erholen.¹⁰ Ein zuverlässiger und detaillierter Informationsaustausch über Vorfälle mit Drohnen in der EU, der über den bereits in bestimmten kritischen Bereichen wie Flughäfen stattfindenden

⁸ Nutzung der EU-Plattform CIRCABC, die im Rahmen des [ISA²-Programms](#) der Europäischen Kommission unterstützt wird, das Interoperabilitätslösungen für europäische öffentliche Verwaltungen fördert.

⁹ Die (informelle) Arbeitsgruppe des Strafverfolgungsnetzes (Law Enforcement Network Working Group – LENWG), in der die Kommission den Vorsitz führt, trat am 20. März 2023 zum ersten Mal zusammen, um die Zusammenarbeit zwischen den von der GD HOME finanzierten Netzen zu verbessern. Die LENWG könnte nach einem zwölfmonatigen Evaluierungszeitraum in eine echte Expertengruppe der Kommission umgewandelt werden.

¹⁰ Die Agentur der Europäischen Union für Flugsicherheit (EASA) veröffentlichte im März 2021 eine Reihe von Leitlinien für den Umgang mit Drohnenfällen auf Flughäfen: [Drone Incident Management at Aerodromes \(Management von Drohnenfällen auf Flughäfen\)](#).

Austausch hinausgeht, ist für die Förderung von fundierten Unterstützungsmaßnahmen und Politikgestaltung auf EU-Ebene unerlässlich. In folgenden Bereichen besteht ein erhebliches Potenzial zur Verbesserung des Informationsaustauschs, wobei die Vertraulichkeit der Ermittlungen in vollem Umfang gewahrt bleibt: i) von Betreibern nicht kooperativer Drohnen angewandte Methoden, ii) spezifische Bedrohungsmuster, iii) ermittelte potenzielle Risiken. Die Kommission hat den Mitgliedstaaten eine Vorlage für die Meldung von Drohnenvorfällen zukommen lassen, um den Austausch solcher Informationen über Vorfälle zu erleichtern und zu vereinheitlichen. Zur weiteren Verbesserung der Qualität und Häufigkeit des Informationsaustauschs wird die Kommission die Möglichkeit prüfen, eine **digitale Plattform mit Informationen über Drohnenvorfälle** für die zuständigen Behörden einzurichten. Sie könnte dazu dienen, schwere Sicherheitsvorfälle in der EU, an denen Drohnen beteiligt sind, angemessen festzustellen und zu erfassen. Dies kann auch die Cyber-Dimension umfassen, da Drohnen nicht nur zur visuellen, sondern auch zur digitalen Aufklärung eingesetzt werden. Diese Plattform stünde im Einklang mit den bestehenden Meldepflichten gemäß der Verordnung (EU) Nr. 376/2014¹¹ und würde sich nicht mit bestehenden Maßnahmen überschneiden.

Die Kommission wird auch regelmäßige vertrauliche Sitzungen abhalten, um den Austausch von Erkenntnissen aus Vorfällen in einem geeigneten Format zu fördern.

Zentrale Maßnahmen in Bezug auf den Gemeinschaftsaufbau und den Informationsaustausch

- **Die Kommission wird eine Expertengruppe einsetzen, die sich aus Experten der Mitgliedstaaten und anderen Interessenträgern im Bereich der Drohnenabwehr zusammensetzt.**
- **Die Kommission wird die Möglichkeit der Entwicklung einer digitalen Plattform mit Informationen über Drohnenvorfälle prüfen.**
- **Die Kommission wird regelmäßige Sitzungen veranstalten, um den Austausch von Verschlussachen zwischen den Mitgliedstaaten über schwere Sicherheitsvorfälle mit Drohneneinsatz zu erleichtern.**

B. Erprobung von Drohnenabwehrsystemen: Ermittlung und Erprobung von Lösungen

Die Mitgliedstaaten und lokalen Behörden können aus einem breiten Spektrum von auf dem Markt verfügbaren kommerziellen Cyber-Lösungen und anderen Lösungen zur Drohnenabwehr wählen. Diese Entscheidung ist vor allem für lokale Stellen, die nicht über ausreichende technische Möglichkeiten verfügen, eine Herausforderung. Die Kommission wird den Behörden der Mitgliedstaaten im Rahmen der speziellen Expertengruppe für Drohnenabwehr und der Arbeit der Gemeinsamen Forschungsstelle (Joint Research Centre – JRC) der Kommission Beratung und Orientierungshilfe anbieten, damit sie die für ihre operativen Anforderungen richtige Wahl treffen können.

2019 wurden auf EU-Ebene Maßnahmen zur Erprobung von Drohnenabwehrsystemen eingeleitet. Damit soll eine gemeinsame Methodik zur Bewertung von Systemen entwickelt werden, die von Strafverfolgungsbehörden und anderen öffentlichen Stellen zur Erkennung, Verfolgung und Identifizierung potenziell böswilliger Drohnen angewandt werden kann. Eine zentrale Säule dieser

¹¹ Verordnung (EU) Nr. 376/2014 des Europäischen Parlaments und des Rates vom 3. April 2014 über die Meldung, Analyse und Weiterverfolgung von Ereignissen in der Zivilluftfahrt, zur Änderung der Verordnung (EU).

Aktivitäten bildet das Projekt COURAGEOUS¹² (2021–2024), das aus dem EU-Fonds für die innere Sicherheit – Polizei (ISF-Polizei) finanziert wird. Die Leitung von COURAGEOUS obliegt der Königlichen Militärakademie Belgiens, und folgende Aufgaben sind damit verbunden: i) Ermittlung relevanter Standardszenarien für die Erprobung von Drohnenabwehrsystemen, ii) Ausarbeitung von Funktions- und Leistungsanforderungen, iii) Entwicklung einer Methodik für die Durchführung der Erprobung. Im Rahmen des Projekts wird auch die Leistung von Sensoren und integrierten Systemen getestet. Die Ergebnisse des Projekts werden laufend den Mitgliedstaaten sowie ausgewählten Partnerländern und internationalen Organisationen übermittelt. Die Kommission und das COURAGEOUS-Konsortium werden den Mitgliedstaaten nach Abschluss des Projekts Optionen vorlegen, um die Nachhaltigkeit des Projekts zu gewährleisten, und eine **Methodik für Anlagen zur Erprobung der Drohnenabwehr** in den Mitgliedstaaten empfehlen.

Die für Drohnenabwehrsysteme relevanten technologischen Entwicklungen schreiten rasch voran. Flankierend zu den Erprobungsmaßnahmen müssen daher ständig Trends beobachtet werden, um sowohl die vielversprechendsten Lösungen als auch mögliche neue Herausforderungen im Zusammenhang mit der Entwicklung von Drohnenabwehrsystemen zu ermitteln. Die JRC hat Kapazitäten aufgebaut, um diese Beobachtung durchzuführen und diese neuen Herausforderungen zu ermitteln. Dies kommt den Mitgliedstaaten zugute und liefert wertvollen Input für Erprobungsinitiativen auf EU-Ebene. Die Informationen werden über geeignete Kanäle, insbesondere über die Expertengruppe, weitergegeben.

Die Normung ist ein Instrument zur Harmonisierung technologischer Lösungen. Im Rahmen des Projekts COURAGEOUS wurden spezifische Empfehlungen zur Vornormung erarbeitet, auf deren Grundlage die Durchführbarkeit – und Erforderlichkeit – der Einleitung von Normungsprozessen weiter geprüft werden kann. Auf EU-Ebene wurden gute Fortschritte bei der Entwicklung freiwilliger Leistungsanforderungen für Detektionsgeräte außerhalb der Luftfahrt (z. B. für Röntgengeräte und Metalldetektoren¹³) erzielt. Die Kommission wird nun gemeinsam mit Experten aus den Mitgliedstaaten und der Luftfahrtbranche **freiwillige Leistungsanforderungen** für Drohnenabwehrsysteme ausarbeiten, die gegebenenfalls mit den Bestimmungen des Rechtsakts zur Cybersicherheit¹⁴ in Einklang stehen. Die Schaffung eines Zertifizierungsverfahrens für Drohnenabwehrsysteme sollte ein mittelfristiges Ziel bleiben. Gegebenenfalls werden auch hybride Normen für Verwendungszwecke im Zivil- und Verteidigungsbereich in Betracht gezogen.

Ein weiteres Schlüsselement ist die Normung und Zertifizierung der Cybersicherheit von Drohnenabwehrsystemen, insbesondere im Fall von Anbietern aus Drittländern. Derzeit ist noch unklar, wie gut die von bestimmten Detektionssystemen erfassten Daten geschützt sind. Darüber hinaus ist es wichtig, das Hacken und die missbräuchliche Nutzung von Drohnenabwehrsystemen so weit wie möglich dadurch zu verhindern, dass die Cyberresilienz ihrer Komponenten gewährleistet wird.

Die Kommission hat im September 2022 einen Vorschlag für eine Verordnung über die Cyberresilienz¹⁵ angenommen, der darauf abzielt, allgemeine Cybersicherheitsvorschriften für Produkte mit digitalen Komponenten – sowohl Hardware als auch Software –, die Zugang zum Binnenmarkt erhalten, aufzustellen. Mit der vorgeschlagenen neuen Verordnung sollen verbindliche

¹² <https://courageous-isf.eu>

¹³ Empfehlung der Kommission betreffend die freiwilligen Leistungsanforderungen für im öffentlichen Raum genutzte Röntgengeräte, C(2022) 4179.

¹⁴ Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik.

¹⁵ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.

Cybersicherheitsanforderungen für diese Produkte eingeführt werden. Zu diesen Anforderungen gehören Cybersicherheit durch Technikgestaltung und durch entsprechende Voreinstellungen sowie Anforderungen zur Behandlung von Schwachstellen. Wie von der Kommission vorgeschlagen, würden Drohnensysteme, die nicht ausschließlich für Zwecke der nationalen Sicherheit oder für militärische Zwecke entwickelt wurden und die nicht bereits nach der Verordnung (EU) 2018/1139 zertifiziert sind, als Produkte mit digitalen Elementen unter diese neuen Vorschriften fallen, mit Ausnahme derjenigen, die ausschließlich für Zwecke der nationalen Sicherheit oder der Verteidigung entwickelt wurden.

Zentrale Maßnahmen in Bezug auf die Erprobung von Drohnenabwehrsystemen

- **Die Kommission wird aufbauend auf den Ergebnissen des Projekts COURAGEOUS an der Einführung einer einheitlichen Methodik für die Durchführung der Erprobung von Drohnenabwehrsystemen arbeiten.**
- **Die JRC wird einen Jahresbericht über die technischen Entwicklungen im Bereich der Drohnenabwehrtechnik erstellen.**
- **Die Kommission wird in Zusammenarbeit mit den einschlägigen Expertengruppen, etwa den Strafverfolgungsnetzen ENLETS, HRSN und AIRPOL, eine Reihe freiwilliger Leistungsanforderungen für Drohnenabwehrsysteme ausarbeiten.**

C. Praktische Leitlinien und operative Unterstützung

Die Abwehr von Bedrohungen durch nicht kooperative Drohnen wurde bereits in einer Reihe von Veröffentlichungen der JRC als eine Priorität genannt, etwa in den Leitlinien zum Schutz des Sicherheitsperimeters um Gebäude¹⁶ und in der speziellen Studie über von Drohnen transportierte Sprengladungen¹⁷. Darüber hinaus wird in der jüngsten Veröffentlichung¹⁸ über das Konzept der konzeptionsintegrierten Sicherheit (Security by Design) hervorgehoben, wie wichtig es ist, von Anfang an in der Planungs- und Entwurfsphase eines Projekts verhältnismäßige, zweckmäßige und multifunktionale Schutzmaßnahmen in ein durchdachtes Konzept zu integrieren, einschließlich Maßnahmen zur Abwehr von Angriffen, bei denen Drohnen eingesetzt werden.

Zudem enthält das EASA-Handbuch *Drone Incident Management at Aerodromes* eine Anleitung zur Entwicklung geeigneter Vorkehrungen und Verfahren, die als Grundlage für Systeme zur schnellen, wirksamen und verhältnismäßigen Reaktion auf Vorfälle an Flughäfen dienen sollen. So können Aussetzungen des Flugverkehrs oder die Sperrung des Luftraums bzw. der Start- und Landebahnen vermieden oder auf ein Minimum beschränkt werden, und Flughafenschließungen blieben das letzte Mittel. Die EASA trägt bei ihrer Arbeit den Leitlinien der Internationalen Zivilluftfahrt-Organisation für die Luftsicherheit¹⁹ Rechnung.

¹⁶ Karlos, V. und Larcher, M., Guideline – Building Perimeter Protection (Leitlinien – Perimeterschutz von Gebäuden), EUR 30346 EN, Amt für Veröffentlichungen der Europäischen Union, Luxemburg, 2020.

¹⁷ Die Bedrohung durch mit Sprengstoff beladene Drohnen wurde von der JRC untersucht in: Larcher, M., Karlos, V., Valsamos, G., Solomos, G.: Scenario study: drones carrying explosives (Szenariostudie: Drohnen mit Sprengstoff), JRC107683, 2018.

¹⁸ Europäische Kommission, Security by Design: Protection of public spaces from terrorist attacks (Konzeptionsintegrierte Sicherheit: Schutz des öffentlichen Raums vor Terroranschlägen), JRC131172, 2022.

¹⁹ Das ICAO-Handbuch für Luftsicherheit ([ICAO Aviation Security Manual](#), Doc 8973 – Restricted) enthält Leitlinien für die Anwendung der Normen und Verfahrensempfehlungen (Standards and Recommended Practices – SARPs) und dient den Mitgliedstaaten als Hilfestellung bei der Umsetzung von Anhang 17 des Abkommens von Chicago.

Die JRC hat zwei neue Handbücher ausgearbeitet:

- ***Protection against Unmanned Aircraft Systems: Handbook on UAS protection of Critical Infrastructure and Public Space – A five Phase approach for C-UAS stakeholders*** (Schutz vor unbemannten Luftfahrzeugsystemen: Handbuch zum Schutz kritischer Infrastrukturen und des öffentlichen Raums vor unbemannten Luftfahrzeugsystemen – Ein fünfstufiger Ansatz für Interessenträger im Bereich der Drohnenabwehr)
- ***Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites*** (Schutz vor unbemannten Luftfahrzeugsystemen: Handbuch zur Bewertung von Drohnenrisiken und zu Grundsätzen zur physischen Absicherung von Gebäuden und Standorten)

Im Bereich der **Schulungen** wurde im Rahmen des EU-finanzierten Projekts DroneWISE²⁰ ein Paket mit Kommando-, Kontroll- und Koordinierungsstrategien zur Drohnenabwehr für Ersthelfer ausgearbeitet. Im Rahmen des Projekts wurden auch zehn Schulungsmodulare, ein Handbuch und ein Online-Schulungsportal erstellt. Diese Schulungsmodulare wurden in den Lehrplan der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) aufgenommen. Skyfall war ein weiteres ISF-Projekt, das sich mit Schulungen zum Thema Drohnenabwehr befasste. Das Schulungsangebot muss auf private Sicherheitsdienstleister, insbesondere auf solche, die für den Schutz kritischer Infrastrukturen zuständig sind, ausgeweitet werden.

Im Kommissionsprogramm „**EU-Sicherheitsberater**“ (**EU protective security adviser – EU PSA**)²¹ ist ein eigener Abschnitt der Drohnenabwehr gewidmet und beinhaltet Folgendes: i) eine spezifische Schwachstellenbewertung für Hochrisikoeinrichtungen und -infrastrukturen, ii) praktische Empfehlungen für den Umgang mit der Bedrohung durch Drohnen, iii) praktische Empfehlungen zum Umgang mit dem Einsatz von Drohnen-Detektionsgeräten bei Hochrisikoereignissen. Die Kommission wird prüfen, ob ein EU-Pool für Drohnenabwehrausrüstung zur Unterstützung der Mitgliedstaaten bei Großveranstaltungen eingerichtet werden sollte.

Übungen wie die mit dem Strafverfolgungsnetz auf EU-Ebene organisierten tragen zur operativen Abwehrbereitschaft in verschiedenen Bereichen der inneren Sicherheit bei. Gegebenenfalls wird die Kommission mit den einschlägigen Netzen zusammenarbeiten, um in künftigen Übungen Elemente der Drohnenabwehr zu berücksichtigen. Dies wird dazu beitragen, den Kenntnisstand und den Austausch bewährter Verfahren zu verbessern und andere Lösungsansätze zu verfolgen. Eine zuverlässig sichere Kommunikation zwischen den verschiedenen Behörden ist eine Voraussetzung für eine wirksame Reaktion auf Bedrohungen, die von Drohnen ausgehen. Die Abwehr von Bedrohungen, die von Drohnen ausgehen, wird daher Teil der künftigen Übungsplanung sein, die im Rahmen des EU-finanzierten Vorbereitungsprojekts BroadEU.Net durchgeführt wird, bei dem die Grundlage des künftigen EU-Systems für kritische Kommunikation²² getestet wird. Darüber hinaus könnten gemeinsame Übungen durchgeführt werden, an denen Experten für Cybersicherheit und Drohnensicherheit teilnehmen, die von Drohnen ausgehende Cyberrisiken sowie digitale Lösungen zur Neutralisierung von Drohnen behandeln.

²⁰ <https://dronewise-project.eu/>

²¹ https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en

²² Das EU-System für kritische Kommunikation wird eine sichere Breitbandinfrastruktur bieten, um die grenzüberschreitende Interoperabilität der in der Strafverfolgung und im Katastrophenschutz genutzten Kommunikationssysteme im Schengen-Raum zu gewährleisten.

Zentrale Maßnahmen in Bezug auf praktische Leitlinien und operative Unterstützung

- **Die JRC wird zwei Handbücher als Teil des Pakets zur Drohnenabwehr veröffentlichen.**
- **Die Kommission wird in Zusammenarbeit mit den einschlägigen Agenturen die Ausweitung bestehender Schulungen zur Drohnenabwehr auf den privaten Sicherheitssektor unterstützen.**
- **Sie wird in Kooperation mit den Strafverfolgungsnetzen die Komponenten der Drohnenabwehr in die Planung von Übungen einbeziehen.**

D. Forschung und Innovation

Die EU setzt die Finanzierung ihres Sicherheitsforschungsprogramms im Rahmen von **Horizont Europa (2021-2027)**²³ fort. Rund 50 % der gesamten öffentlichen Mittel, die in der EU und ihren Mitgliedstaaten in den Bereich der Sicherheit investiert werden, entfallen auf dieses Sicherheitsforschungsprogramm. Diese Sicherheitsforschung, die einen strategischen Beitrag zu verschiedenen sicherheitspolitischen Prioritäten der EU leistet, befasst sich auch bereits mit den von Drohnen ausgehenden Bedrohungen. Hervorzuheben sind beispielsweise das Projekt ALADDIN, das Lösungen zur Erkennung und Neutralisierung von Drohnen in Flugbeschränkungsgebieten²⁴ liefert, oder das Projekt 7SHIELD, das sich mit der Entwicklung von Lösungen zur Drohnenabwehr für Bodensegmente kritischer Weltrauminfrastrukturen befasst. Im Rahmen des Projekts ALFA wurde auch ein System zur Erkennung und Verfolgung von Drohnen entwickelt, die für den Schmuggel eingesetzt werden.²⁵ Diese Initiativen für Forschung und Innovation können unter Horizont Europa fortgesetzt, validiert oder durch Maßnahmen im Rahmen von ISF-Polizei ergänzt werden.

Künftig wird die Kommission den systematischeren Austausch relevanter Projektergebnisse mit den einschlägigen Interessenträgern fördern, auch über die Gemeinschaft für europäische Forschung und Innovation im Dienste der Sicherheit²⁶. Dadurch könnte der spezifische Datenaustausch weiter ausgebaut werden. Ferner könnten so die Anforderungen der Nutzer effizienter erfasst und zur Steuerung der Innovation an die Luftfahrtbranche weitergeleitet werden. Darüber hinaus wird der systematische Austausch von Projektergebnissen dazu beitragen, einen strukturierten Dialog mit den Mitgliedstaaten und Interessenträgern zur Ermittlung vielversprechender Technologien, Instrumente und Lösungen zu ermöglichen, die von einer Gruppe von Behörden der Mitgliedstaaten übernommen werden könnten. Die Kommission wird in diesem Zusammenhang gemeinsam mit den Mitgliedstaaten²⁷ folgende Möglichkeiten prüfen: i) Schaffung eines eigenständigen Forschungsbereichs zu Drohnenabwehrlösungen in den künftigen Arbeitsprogrammen von Horizont Europa, ii) Unterstützung

²³ Bis Ende 2020 erfolgte die Finanzierung der Sicherheitsforschung und -innovation im Rahmen von Horizont 2020 und des 7. Forschungsrahmenprogramms.

²⁴ <https://cordis.europa.eu/project/id/740859>

²⁵ ALFA bildet auch die Grundlage für das ISF-Projekt COURAGEOUS und die entsprechenden Erprobungsaktivitäten.

²⁶ Die Gemeinschaft für Europäische Forschung und Innovation im Dienste der Sicherheit (CERIS) bringt Akteure der Sicherheitsforschung – von politischen Entscheidungsträgern über Endnutzer, Hochschulen, Luftfahrtbranche bis hin zur zivilen Sicherheit – zusammen: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en.

²⁷ Im Rahmen des Programmausschusses „Zivile Sicherheit für die Gesellschaft“ des Programms Horizont Europa.

spezifischer innovativer Systeme durch vorkommerzielle Auftragsvergabe²⁸. Dies steht in vollem Einklang mit dem auf Fähigkeiten ausgerichteten Ansatz, der in der Arbeitsunterlage der Kommissionsdienststellen zum Thema Verbesserung der Sicherheit durch Forschung und Innovation²⁹ dargelegt ist.

Die Stärkung von Synergien bei Drohnenabwehrlösungen zwischen ziviler Sicherheit, Verteidigung und Raumfahrtindustrie in Europa ist von entscheidender Bedeutung. Ziel sollte es sein, Synergien bei Drohnen- und Drohnenabwehrtechnologien zwischen den drei Sektoren zu fördern.³⁰ In der Praxis bedeutet die Stärkung dieser Synergien, dass Verteidigungsprojekte von innovativen Entwicklungen im zivilen Bereich profitieren können, während Entwicklungen im Verteidigungsbereich der zivilen Luftfahrt zugutekommen können.

Über den **Europäischen Verteidigungsfonds (EVF)** und seine Vorläuferprogramme werden kooperative, grenzüberschreitende Forschung und Entwicklung im Verteidigungsbereich gefördert und unterstützt. Der EVF ergänzt und verstärkt die Anstrengungen der Mitgliedstaaten und fördert die Zusammenarbeit zwischen Unternehmen und Forschungsakteuren aller Größenordnungen und aus allen Mitgliedstaaten der EU. Über die Vorläuferprogramme des EVF wurden im Rahmen verteidigungsbezogener Forschung und Entwicklung bereits Projekte zur Drohnenabwehr finanziert.

Das EVF-Arbeitsprogramm für 2023 enthält eine Maßnahme zur Drohnenabwehr³¹ mit veranschlagten Mitteln in Höhe von 43 Mio. EUR. Ziel der Maßnahme ist die Entwicklung von Hardware- oder Softwaremodulen für eine umfassende mobile Lösung zur Abwehr eines breiten Spektrums von Drohnen, einschließlich Schwärmen.

Das wichtigste erwartete Ergebnis der EVF-Unterstützung im Bereich der Drohnenabwehr im Zeitraum 2021–2027 ist ein entwickelter Prototyp für eine Drohnenabwehrlösung, dem eine künftige gemeinsame Beschaffung auf EU-Ebene folgen könnte. Technologische Herausforderungen im Bereich der Drohnenabwehr werden im Rahmen des EU-Innovationsprogramms im Verteidigungsbereich (EUDIS) behandelt. Darüber hinaus umfasst EUDIS einen Bereich für Inkubatoren mit doppeltem Verwendungszweck, um eine bessere Zusammenarbeit zwischen dem zivilen und dem militärischen Bereich zu fördern und die technologische Ausreifung und Anpassung voranzutreiben.

Ein weiterer wichtiger Pfeiler für die Innovation – und insbesondere für die angewandte Forschung zur Abwehr von Bedrohungen, die von Drohnen ausgehen – ist die Arbeit der JRC. Im Rahmen des JRC-Projekts „Drone C-UAS“ wird die JRC Technologien für aktive und passive Gegenmaßnahmen prüfen und untersuchen, wie diese Technologien eingesetzt werden können, um die Sicherheit des öffentlichen Raums und kritischer Infrastrukturen zu gewährleisten.

²⁸ Die vorkommerzielle Auftragsvergabe (pre-commercial procurement – PCP) ist ein in der PCP-Mitteilung (C(2007) 799 final) vom 14.12.2007 vorgestellter Ansatz für die öffentliche Auftragsvergabe von Dienstleistungen im Bereich Forschung und Entwicklung (FuE). Sie ist ein wichtiges Instrument zur Förderung der Innovation, da sie den öffentlichen Sektor in die Lage versetzt, die Entwicklung neuer Lösungen auf seinen Bedarf auszurichten.

²⁹ Arbeitsunterlage der Kommissionsdienststellen „Enhancing security through research and innovation“, SWD(2021) 422 final vom 15.12.2021.

³⁰ SWD(2022) 362 vom 10.11.2022. Wie im Fortschrittsbericht über die Umsetzung des Aktionsplans für Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie (Maßnahme 9) beschrieben.

³¹ Durchführungsbeschluss C(2023) 2296 der Kommission vom 29.3.2023 zur Finanzierung des mit der Verordnung (EU) 2021/697 des Europäischen Parlaments und des Rates eingerichteten Europäischen Verteidigungsfonds und zur Annahme des Arbeitsprogramms für 2023 – Teil II).

Dazu wird die JRC in einem ersten Schritt ein **Living Lab** einrichten, um Drohnenabwehrtechnologien zu untersuchen und zu prüfen, wie diese in realen Umgebungen eingesetzt werden können. Der Laboraufbau umfasst die Planung, Vorbereitung und Umsetzung einer Lösung. Außerdem werden die Erkennung, Verfolgung, Identifizierung und Neutralisierung sowie die Einbindung von Interessenträgern und Verfahren behandelt. Der Umsetzungsumfang des Living Labs wird auch die Integration in bemannte und unbemannte Verkehrsmanagementsysteme, insbesondere U-Space, umfassen.³² Im Rahmen des Living Labs wird auch untersucht, wie maschinelles Lernen und künstliche Intelligenz integriert werden können, um die Gesamtleistung einer Drohnenabwehlösung zu verbessern.

Mittelfristig soll dieses Living Lab der JRC zu einem **Kompetenzzentrum für die Drohnenabwehr** ausgebaut werden.

Vorrangige Maßnahmen zur optimalen Nutzung von Forschung und Innovation

- **Die Kommission und die Mitgliedstaaten werden über den künftigen Bedarf an neuen Drohnenabwehlösungen entscheiden, der im Rahmen der einschlägigen europäischen Forschungs- und Innovationsprogramme, insbesondere Horizont Europa, gedeckt werden soll.**
- **Die Kommission und die Mitgliedstaaten werden eine Liste vielversprechender Lösungen zur Drohnenabwehr erstellen und die Durchführbarkeit einer vorkommerziellen Auftragsvergabe für einige dieser Lösungen prüfen.**
- **Die Kommission wird Konzepte, Technologien und Lösungen ermitteln, die in die Entwicklung der Verteidigungskapazitäten einfließen sollen, und Projekte unterstützen, die darauf abzielen, diese Konzepte, Technologien und Lösungen in zivilen Sektoren zu verbreiten.**
- **Die JRC wird das Living Lab zu einem Kompetenzzentrum für Drohnenbekämpfung weiterentwickeln.**

E. Finanzielle Unterstützung

Die Kommission wird weiterhin einschlägige Maßnahmen zur Drohnenabwehr finanziell unterstützen, in erster Linie über den ISF, aber auch im Rahmen des Instruments für finanzielle Hilfe im Bereich Grenzverwaltung und Visumpolitik (BMVI) und des Programms Horizont Europa (für forschungs- und innovationsbezogene Maßnahmen).

Im Rahmen der Thematischen Fazilität des ISF wird Folgendes unterstützt: i) die Europäischen Strafverfolgungsnetze, ii) die diesbezügliche Arbeit der JRC, iii) die neue Expertengruppe zur Drohnenabwehr, iv) die Einrichtung einer Plattform für den Informationsaustausch. Die Kommission finanziert bereits Projekte zur Erprobung und Validierung von Systemen zur Erkennung und Ortung von Drohnen, die die EU-Außengrenzen illegal überschreiten. Diese Projekte beruhen auf den Ergebnissen früherer EU-finanzierter Forschungsprojekte.³³

³² Durchführungsverordnung (EU) 2021/664 der Kommission über einen Rechtsrahmen für den U-Space. Der Begriff „U-Space“ wurde zur Beschreibung des Verkehrsmanagements unbemannter Luftfahrzeuge gewählt, um die sichere Interaktion mit anderen Einheiten zu gewährleisten, die in städtischen Gebieten und an anderen Orten denselben Raum nutzen.

³³ Beispiele hierfür sind Projekte, die im Rahmen der spezifischen Maßnahmen des BMVI zu folgenden Themen finanziert werden: i) Innovation für See-/Küsten- und/oder Landgrenzen, ii) Frontex. Einige Projekte, die im

Im Rahmen der Thematischen Fazilität des ISF wird die Kommission im ersten Halbjahr 2024 eine **Aufforderung zur Einreichung von Vorschlägen** veröffentlichen, die speziell auf die Unterstützung der Einführung von Drohnenabwehrlösungen mit hohem Potenzial für eine Übernahme abzielt.

Die Mitgliedstaaten werden aufgefordert, diese Mitteilung umzusetzen und den Erkenntnissen aus der EU-finanzierten Forschung im Rahmen ihrer ISF-Programme in Drohnenabwehrlösungen Rechnung zu tragen.

Zentrale Maßnahmen in Bezug auf die finanzielle Unterstützung

- **Die Kommission wird im Rahmen der Arbeitsprogramme der Thematischen Fazilität des ISF für den Zeitraum 2026–2027 eine Aufforderung zur Einreichung von Vorschlägen für Drohnenabwehrlösungen veröffentlichen.**
- **Die Mitgliedstaaten werden aufgefordert, ihre ISF-Programme für den Zeitraum 2021–2027 in vollem Umfang zu nutzen, um effiziente Lösungen zur Abwehr von Drohnen zu ermitteln und umzusetzen.**

F. Prüfung regulatorischer Maßnahmen

Die EU hat zwar die rechtmäßige Nutzung von Drohnen geregelt, doch gibt es auf EU-Ebene derzeit keine spezifischen Vorschriften zur Drohnenabwehr, die einen gemeinsamen harmonisierten Rahmen für die Behörden der Mitgliedstaaten, die Betreiber und die Hersteller bilden. Obgleich die (in dieser Mitteilung bereits genannten) unverbindlichen EASA-Leitlinien zu Drohnenvorfällen auf Flughäfen von der Luftfahrtbranche positiv aufgenommen wurden, sind sie aufgrund ihres beratenden Charakters und ihres begrenzten Anwendungsbereichs unzureichend, um die von nicht kooperativen Drohnen ausgehende Bedrohung zu mindern. Die Kommission wird angesichts der zunehmenden Dringlichkeit, den unerlaubten Einsatz von Drohnen wirksam zu verhindern, in enger Zusammenarbeit mit Experten aus den Mitgliedstaaten weiter den künftigen Bedarf an legislativen oder nichtlegislativen Maßnahmen analysieren. Dafür wird sie eigens eine **Studie zur Bestandsaufnahme** in Auftrag geben, um das derzeitige Regelungsumfeld zu ermitteln. Diese Studie sollte auch dem ICAO-Rahmen und den Entwicklungen Rechnung tragen und darauf eingehen, dass Vorschriften zur Abwehr potenzieller Bedrohungen, die von Drohnen ausgehen, den rechtmäßigen Betrieb, einschließlich der Aktivitäten organisierter Freizeitpiloten, nicht ungebührlich behindern sollten.

Für Flughäfen in der EU gelten detaillierte und umfassende Sicherheitsvorschriften, die auch die Bedrohung durch Drohnen einschließen. Zur Verbesserung der Resilienz von Luftverkehrsbehörden und Flughäfen gegenüber den von Drohnen ausgehenden Risiken und anhand eines faktengestützten Ansatzes wird die Kommission in Zusammenarbeit mit den Mitgliedstaaten im Rahmen einer Sicherheitsrisikobewertung **potenzielle zusätzliche Schwachstellen beim Schutz vor nicht kooperativen Drohnen ermitteln, die möglicherweise Änderungen der Rechtsvorschriften erforderlich machen.**

Rahmen der spezifischen Maßnahme zur Innovation für See-/Küsten- und/oder Landgrenzen finanziert werden, konzentrieren sich auf die Erprobung innovativer Überwachungstechnologien. Ferner gibt es eine spezifische Maßnahme für den Erwerb und die Bereitstellung von Ausrüstung für den Einsatz durch die europäischen Grenzbehörden, um Drohnen, die im Zuge illegaler oder krimineller Aktivitäten die Grenzen überschreiten, zu erkennen und zu orten. Im Rahmen dieser spezifischen Maßnahme können die Mitgliedstaaten zwei Drohnenabwehrsysteme beschaffen. Als EU-Mehrwert muss auf Antrag von Frontex im Rahmen der jährlichen bilateralen Verhandlungen die im Rahmen der spezifischen Maßnahmen erworbene technische Ausrüstung für einen Zeitraum von bis zu vier Monaten pro Jahr für die gemeinsamen Operationen von Frontex zur Verfügung gestellt werden.

In diesem Zusammenhang ist ein strukturierter Dialog mit der Luftfahrtbranche und den Drohnenherstellern über Maßnahmen im Bereich der konzeptionsintegrierten Sicherheit erforderlich (z. B. robuste Systeme gegen Spoofing, Fähigkeitsbeschränkungen, gemeinsame Nutzung von Kommunikationsprotokollen und Aktualisierungen von Drohnenabwehrdatenbanken).

Zentrale Maßnahmen in Bezug auf die Prüfung regulatorischer Maßnahmen

- **Die Kommission wird eine Studie zur Bestandsaufnahme in Auftrag geben, um den Regulierungsbedarf und das Potenzial für eine Harmonisierung der Rechtsvorschriften und Verfahren der Mitgliedstaaten zu ermitteln.**
- **Sie wird anhand eines faktengestützten Ansatzes eine Bewertung des Luftsicherheitsrisikos in Bezug auf Drohnen vornehmen, um potenzielle zusätzliche Schwachstellen von Flughäfen zu ermitteln, die möglicherweise Änderungen der Rechtsvorschriften erforderlich machen.**
- **Die Kommission wird einen strukturierten Dialog mit der Luftfahrtbranche darüber führen, ob zusätzliche spezifische Maßnahmen zur Sicherheit von Drohnen erforderlich sind und welcher Art diese sein könnten.**

III. WEITERES VORGEHEN

Damit die rasche technologische Entwicklung und die wachsende Zahl von Drohnen nicht zu einer unkontrollierten Zunahme der Bedrohungen durch nicht kooperative Drohnen führen, muss die Zusammenarbeit auf EU-Ebene auf der Grundlage der in dieser Mitteilung dargelegten umfassenden EU-Politik zur Drohnenabwehr verstärkt werden. Dazu werden die laufenden Tätigkeiten auf EU-Ebene fortgesetzt und durch die in dieser Mitteilung aufgeführten zentralen Maßnahmen ergänzt, die in den kommenden Jahren durchgeführt werden.

Die in dieser Mitteilung dargelegten Maßnahmen werden sich auf den Zeitraum bis 2030 erstrecken. 2027 wird die Expertengruppe eine Halbzeitbilanz ziehen, und spätestens 2030 soll das EU-Programm zur Drohnenabwehr einer vollständigen Überarbeitung unterzogen werden.